

**THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF
MICHIGAN**

RICHARD JOURNAGIN,
individually and on behalf of all
others similarly situated,

Plaintiff,

v.

MORLEY COMPANIES, INC.,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Richard Journagin (“Plaintiff”) brings this Class Action Complaint against Morley Companies, Inc., (“Morley” or “Defendant”), individually and on behalf of all others similarly situated (“Class Members”), and alleges, upon personal knowledge as to his own actions and his counsels’ investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive information that Plaintiff and Class Members entrusted to it. This sensitive information, includes, without limitation, names, addresses, Social Security numbers, dates of birth, driver’s license numbers, client and/or member identification numbers, medical diagnostic and treatment information, and health insurance information including medications, conditions,

and providers (collectively, “personally identifiable information” or “PII”).¹ Plaintiff alleges that Defendant failed to comply with industry standards to protect information systems that contain PII, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII and PHI had been accessed and potentially acquired by an unauthorized third-party. Plaintiff seeks, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised, to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future, to destroy information no longer necessary to retain for purposes for which the information was first obtained from Class Members, and to provide a sum of money sufficient to provide to Plaintiff and Class Members identity theft protective services for their respective lifetimes as Plaintiff and Class Members will be at an increased risk of identity theft due to the conduct of Morley as described herein.

2. Morley is an international provider of business services to Fortune 500 companies. Its services include business process outsourcing, organizing meetings and incentives, and designing, fabricating, and installing exhibits and displays. Morley assists clients in industries including automotive, healthcare, technology, and

¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver’s license number, financial account number).

communications.

3. Plaintiff and Class Members are current and former employees of Morley as well as various clients. Upon information and belief, it appears that customers of Morley's clients were also affected. In the ordinary course of business, Plaintiff and Class Members were regularly required to provide their PII to Morley as a condition of their employment or business relationship.

4. Beginning on August 1, 2021, Morley discovered that it could not access data on its computer systems. After investigation, Morley learned that an unauthorized third party had gained access to files on its services where sensitive PII was stored (the "Data Breach").²

5. In its Notice of Data Breach published on its website on February 2, 2022, Morley advises that the data accessed contained PII.³ However, the Notice provides scant other information, including how long these unauthorized third-parties had access to the sensitive information of Plaintiff and Class Members.⁴

6. Further, Morley has failed to adequately explain why it took six months to begin notifying individuals that their PII had been accessed by an unauthorized third-party.

7. This case involves a breach of a computer system by an unknown third-

² See <https://morleycompanies.com/about/cyber-security-incident/> (last accessed Feb. 21, 2022).

³ *Id.*

⁴ *Id.*

party, resulting in the unauthorized disclosure and potential acquisition of the PII of Plaintiff and Class Members to unknown third-parties. As a result of Defendant's failure to implement and follow basic security procedures, the PII of Plaintiff and Class Members was accessed and/or acquired and is now in the hands of criminals. Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Morley's failures.

8. Additionally, as a result of Defendant's failure to follow federally-prescribed, industry standard security procedures, Plaintiff and Class Members received only a diminished value of the services Defendant was to provide.

9. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access, intrusion, and/or acquisition.

10. Defendant admits that the unencrypted PII and PHI exposed to unauthorized access included names, addresses, Social Security numbers, dates of birth, and various types of medical information including diagnostic and treatment information as well as health insurance documentation.⁵

⁵ *Id.*

11. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers and/or specific, sensitive medical information.

12. The Data Breach occurred due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members. Defendant waited months to report the Data Breach to Plaintiff and Class Members and still maintains as secret the specific vulnerabilities and root causes of the Data Breach. Plaintiff and Class Members also remain unaware of precisely what information was accessed and for how long.

13. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to adequately protect the PII of Plaintiff and Class Members and failure to warn Plaintiff and Class Members of Defendant's inadequate information security practices. Defendant's conduct amounts to negligence and violates federal and state statutes.

14. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity

costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and, significantly (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third-parties to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

15. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

16. Plaintiff Richard Journagin is a citizen and resident of Murfreesboro, Tennessee. Plaintiff is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff's PII and has a legal duty and obligation to protect that information.

17. Defendant Morley Companies, Inc. is a Michigan corporation with its principal place of business at 1 Morley Plaza, Saginaw, Michigan 48603. Morley employs over 2,500 associates nationwide and provides dozens of Fortune 500 companies business services, including processing information for health plans.

18. Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

19. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity, as Plaintiff is a citizen of a state different from Morley.

20. This Court has personal jurisdiction over Defendant named in this action because Defendant is headquartered in Saginaw, Michigan, and conducts substantial business in this District.

21. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

I. Background

22. Defendant is a company that provides business services to other companies. Those services include business process outsourcing, meeting planning, and the creation and display of exhibits. Defendant provides these services to companies in the automotive, chemical, financial, insurance, healthcare, technology,

and communications industries.⁶

23. Plaintiff and Class Members include current and former employees of Morley as well as various clients. Plaintiff and Class Members were required to provide Morley with their PII as part of their relationship with Morley. Plaintiff and Class Members entrusted this sensitive and confidential information to Defendant to store and manage. This sensitive and confidential information included, without limitation, their names, addresses, Social Security numbers, and dates of birth, as well as medical treatment and diagnosis information and other personal health information, many of which are static, do not change, and can be used to commit myriad financial crimes.

24. Morley promised to provide confidentiality and adequate safety for Plaintiff and Class Members' PII through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements,

25. For example, in its Notice of Privacy Practices, Morley claims:

We understand the critical nature of our clients' data and employ a comprehensive access and security policy to safeguard against unauthorized access. Password-protected door locking mechanisms and strict adherence to data authorization protocols are among the many steps that help secure these important client assets.⁷

26. The PII stored on Morley's servers is sensitive and confidential, and is protected, private medical information. This includes medical treatment information

⁶ See <https://www.morleynet.com/About/> (last visited Feb. 21, 2022).

⁷ See <https://www.morleynet.com/About/Privacy-Policy/> (last visited Feb. 21, 2022).

and other PII that may divulge underlying mental or physical diagnoses, as well as prescription, testing/laboratory results, physician's notes, and other personal health information.

27. Defendant has not yet made Plaintiff and Class Members aware of the extent to which the above referenced records and documentation were accessed and/or acquired or when Morley's data systems were compromised.

28. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

29. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from unauthorized disclosure to third-parties.

II. The Data Breach

30. Defendant admitted in its Notice of Data Breach that an unknown, unauthorized third-party accessed Defendant's data server. Defendant also admitted that an unauthorized third-party accessed files containing sensitive information, including names, Social Security numbers, dates of birth, addresses and medical records.

31. Morley contends that, after discovering the Data Breach on August 1, 2021, it retained a third-party computer forensic specialist to determine the nature

and scope of the incident.⁸ Morley claims that its investigation revealed that the Data Breach was the result of a “ransomware-type malware.”⁹ However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the adequacy of any remedial measures undertaken to ensure a breach does not occur again have not been transparently shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

32. Morley also claims that on January 18, 2022, it “confirmed” that Plaintiff’s and Class Members’ PII was involved in an “incident.”¹⁰

17. Michigan Attorney General Dana Nessel issued a press release on February 11, 2022 regarding the Data Breach.¹¹ The press release, after providing information about the Data Breach, warned:

While the notification letters going to potentially affected individuals are legitimate, bad actors may take the opportunity to use the breach to access additional personal information.

“Watch out for fraudulent emails, phone calls, and text messages seeking personal or banking information in connection to the Morley breach,” Nessel said. “As recipients of the notice will see in Morley’s letter, the company will explain steps to take to protect the information, as well as access to free credit monitoring and identity theft protection services. If you receive other correspondence that asks you do to something like call a number to confirm your personal information, assume it's a scam.”¹²

⁸ See <https://www.mass.gov/doc/assigned-data-beach-number-25888-morley-companies-inc-additional-information/download> (last visited Feb. 21, 2022).

⁹ *Id.*

¹⁰ *Id.*

¹¹ See Department of Attorney General, *AG Nessel Issues Information, Warning Related to Morley Companies Data Breach*, https://www.michigan.gov/ag/0,4534,7-359-92297_47203-577296--,00.html (last visited Feb. 21, 2022).

¹² *Id.*

33. The PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members.

34. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained and stored belonging Plaintiff and Class Members, causing the exposure of this PII.

III. The Health Care Sector is Particularly Susceptible to Data Breaches

35. Defendant was on notice that companies with health care information are routine targets for data breaches.

36. Defendant was also on notice that the FBI has been concerned about data security of health care information. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the health care industry that hackers were targeting them. The warning stated that “[t]he FBI has observed malicious actors targeting health care related systems, perhaps for the purpose of obtaining the Protected Health care Information (PHI) and/or Personally Identifiable Information (PII).”¹³

37. The American Medical Association (“AMA”) has also warned health care companies about the importance of protecting their patients’ confidential

¹³ Jim Finkle, *FBI Warns Health care Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), available at: <https://www.reuters.com/article/us-cybersecurity-health-care-fbi/fbi-warns-health-care-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820> (last visited Jan. 11, 2022).

information:

Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.¹⁴

38. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.¹⁵ In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.¹⁶ That trend continues.

39. The health care sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.¹⁷ Indeed, when compromised, health care related data is among the most sensitive and personally consequential. A report focusing on health care breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about \$20,000," and that the victims were often forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.¹⁸ Almost 50 percent of the

¹⁴ Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), available at: <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals> (last visited Jan. 11, 2022).

¹⁵ Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), available at: <https://www.idtheftcenter.org/post/data-breaches-up-nearly-45-percent-according-to-annual-review-by-identity-theft-resource-center-and-cyberscout/> (last visited Jan. 11, 2022).

¹⁶ Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, available at: <https://www.idtheftcenter.org/2017-data-breaches/> (last visited Sept. 18, 2020).

¹⁷ Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, available at: <https://www.idtheftcenter.org/2018-data-breaches/> (last visited Sept. 18, 2020).

¹⁸ Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), available at:

victims lost their health care coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.¹⁹

40. Health care related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by “bad actors” such as cybercriminals.²⁰ “Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.”²¹

IV. Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.

<https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last visited Feb. 22, 2022).

¹⁹ *Id.*

²⁰ 2019 HIMSS Cybersecurity Survey, available at:

https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Jan. 13, 2022).

²¹ Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, available at: <https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last visited Jan. 13, 2022).

41. Morley acquired, collected, and stored the PII of Plaintiff and Class Members.

42. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

43. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and implicitly relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

V. Securing PII and Preventing Breaches

44. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially outdated information.

45. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

46. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

47. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”²² The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”²³

48. The ramifications of Defendant’s failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

VI. Value of Personal Identifiable Information

49. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.²⁴ Experian reports that a stolen credit or debit card number can sell for \$5 to

²² 17 C.F.R. § 248.201 (2013).

²³ *Id.*

²⁴ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct.16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Jan. 13, 2022).

\$110 on the dark web.²⁵

50. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

51. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.²⁶

52. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not

²⁵ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Jan. 13, 2022).

²⁶ *Identity Theft and Your Social Security Number*, Social Security Administration, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Jan. 13, 2022).

permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

53. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”²⁷

54. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—name, Social Security number, medical records, and potentially date of birth.

55. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²⁸

²⁷ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Jan. 13, 2022).

²⁸ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Jan. 13, 2022).

56. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

57. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft and/or to sell to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

58. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁹

59. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers and medical records, and of the foreseeable consequences that would occur if Defendant's data security system was breached,

²⁹ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Jan. 13, 2022).

including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

60. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

61. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's file servers, amounting to hundreds of thousands of individuals' detailed, personal information and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

62. To date, Defendant has offered Plaintiff and Class Members only one year of identity protection service. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

63. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

VII. Morley Failed to Comply with FTC Guidelines

64. Morley was prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or

affecting commerce.” The FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

65. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.³⁰

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.³¹ The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.

67. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for

³⁰ Federal Trade Commission, *Start With Security: A Guide for Business*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited Jan. 13, 2022).

³¹ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 13, 2022).

security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.³²

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. Defendant failed to properly implement basic data security practices. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

70. Defendant was at all times fully aware of its obligation to protect the PII that Plaintiff and Class Members entrusted to it.

VIII. Plaintiff’s Experience

71. Plaintiff was required to provide his PII to his health insurance company as a condition of receiving health insurance coverage. Upon information and belief, Plaintiff’s health insurance company was a client of on or before August 1, 2021.

³² FTC, *Start With Security*, *supra*.

Defendant possessed Plaintiff's PII at that same time.

72. Plaintiff received Defendant's Notice of Data Breach on or around February 1, 2022. The notice stated that Plaintiff's PII had been improperly accessed by third parties. This PII included his name, health insurance member identification number, date of birth, address, and health insurance information that may have included, among other things, medication, condition or provider information.

73. As a result of receiving the Notice of Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

74. Since the Data Breach, Plaintiff has received a barrage of phone calls on his landline phone, which he had previously provided to his health insurance company, from individuals claiming to be from various unrecognizable pharmacies. Initially, Plaintiff answered several of these phone calls and was asked to take surveys regarding medications and health information. Plaintiff has realized that these calls were not legitimate.

75. The phone calls continued with unbearable frequency throughout the winter of 2021 and January of 2022, so much so that Plaintiff disconnected his telephone number, one which he had since approximately 1990, on or about February 10, 2022.

76. Plaintiff is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

77. Plaintiff stores any documents containing his sensitive PII in a safe and secure location.

78. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted Defendant, which was compromised in and as a result of the Data Breach.

79. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns for the loss of his privacy.

80. Plaintiff has suffered injury arising from the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff's PII has already been misused, upon information and belief, as evidenced by the barrage of health care related phone calls he has received since the Data Breach.

81. Plaintiff has a continuing interest in ensuring that his PII, which remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

82. Plaintiff brings this nationwide class action on behalf of himself and on

behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

83. The Class that Plaintiff seeks to represent is defined as follows:

All United States residents whose PII was maintained on Defendant Morley's computer systems that were compromised in the Data Breach, and who were sent Notice of the Data Breach.

84. Excluded from the Class are the following individuals and/or entities:

Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff members.

85. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

86. Numerosity, Fed. R. Civ. P. 23(a)(1): The members of the Class are so numerous that joinder of all members is impracticable. Plaintiff is informed and believes that the Data Breach affected more than 500,000 individuals. The Class is identifiable within Defendant's records.

87. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and

fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include, without limitation:

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;
- b. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had duties not to use the PII of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
- e. When Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;
- k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and
- m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

88. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

89. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds

generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

90. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

91. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action

treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

92. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the cost of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

93. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant

manageability problems with prosecuting this lawsuit as a class action.

94. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

95. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

96. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

97. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and

safeguarding their PII;

- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;
- e. Whether Defendant breached the implied contract;
- f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,
- i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

98. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 96.

99. Defendant directly or indirectly through its clients required Plaintiff and Class Members to submit sensitive PII as a condition of receiving benefits from Defendant.

100. Morley owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

101. Plaintiff and Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

102. Morley had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

103. Defendant also knew of the serious harms and the types of harm that Plaintiff and the Class Members could and would suffer if the PII were wrongfully disclosed, that disclosure was not fixed, or Plaintiff and the Class were not told about the disclosure in a timely manner.

104. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and Class Members in Defendant's possession was adequately secured and protected.

105. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and Class Members.

106. Defendant's duty to use reasonable security measures arose as a result of the relationship that existed between Defendant and Plaintiff and Class Members. That relationship arose because Plaintiff and Class Members entrusted Defendant with their confidential PII, a necessary and required part of using Defendant's services.

107. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

108. Defendant had a common law duty to prevent foreseeable harm to those whose PII it stored. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices.

109. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of

Defendant's inadequate security practices.

110. Plaintiff and Nationwide Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and Class Members, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Morley knew or should have known that it was more likely than not Plaintiff and Class Members would be harmed.

111. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members.

112. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and Class Members, including basic encryption techniques freely available to Defendant.

113. Plaintiff and Class Members had no ability to protect their PII and PHI that were and remain in Defendant's possession.

114. Defendant was in a position to protect against the harm suffered by

Plaintiff and Class Members as a result of the Data Breach.

115. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

116. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

117. Defendant has admitted that the PII of Plaintiff and Class Members was wrongfully disclosed and/or lost to unauthorized third persons as a result of the Data Breach.

118. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Defendant's possession or control.

119. Defendant improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

120. Defendant failed to heed industry warnings and alerts to provide

adequate safeguards to protect the PII of Plaintiff and Class Members in the face of increased risk of theft.

121. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the PII of Plaintiff and Class Members.

122. Defendant's failure to comply with industry and federal regulations further demonstrates Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting the PII of Plaintiff and Class Members.

123. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

124. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

125. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PII of Plaintiff and Class Members was accessed and/or lost as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

126. Additionally, Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant’s duty in this regard.

127. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

128. Defendant’s violation of Section 5 of the FTC Act constitutes negligence *per se*.

129. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

130. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

131. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosure so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and Class Members; and (viii) present and future costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

132. As a direct and proximate result of Defendant's negligence and negligence *per se* Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety,

emotional distress, loss of privacy, and other economic and non-economic losses.

133. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

134. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

135. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 96 as though fully set forth herein.

136. Plaintiff and Class Members were required to provide their PII, including their names, Social Security numbers, addresses, dates of birth, and various health related information to Defendant as a condition of their use of Defendant's services. By providing their PII, and upon Defendant's acceptance of such information, Plaintiff and all Class Members, on one hand, and Morley on the other

hand, entered into implied-in-fact contracts for the provision of data security.

137. These implied-in-fact contracts obligated Morley to take reasonable steps to secure and safeguard the PII of Plaintiff and Class Members, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen. The terms of these implied contracts are further described in the federal laws, state laws, and industry standards alleged above, and Defendant expressly assented to these terms in their public statements regarding data security described above.

138. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

139. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data and cyber security practices and policies were reasonable and consistent with industry standards.

140. Plaintiff and Class Members would not have provided and entrusted their PII to Defendant in the absence of the implied contract or implied terms between them and Defendant. The safeguarding of the PII of Plaintiff and Class Members was critical to realize the intent of the parties.

141. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their personal information and by failing to provide timely and accurate notice to them that PII was compromised as a

result of the Data Breach.

142. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm

143. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

144. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 96.

145. Defendant benefited financially from receiving the PII of Plaintiff and

Class Members through its contracts with its customers for litigation support services. Defendant understood this benefit.

146. Defendant understood and appreciated that the PII of Plaintiff and Class Members was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

147. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

148. The monies that Defendant received for business services were to be used by Morley, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures in order to secure the PII of Plaintiff and Class Members, upon which Defendant relied.

149. But for Defendant's commitment to maintain privacy and confidentiality, the PII of Plaintiff and Class Members would not have been transferred to and untrusted with Defendant. Indeed, if Morley had informed Plaintiff and Class Members that its data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by the courts, its customers, or consumers.

150. As a result of Defendant's wrongful conduct, Morley has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members. Morley continues to benefit and profit from their retention and use of the PII of

Plaintiff and Class Members while its value to Plaintiff and Class Members has been diminished.

151. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this Complaint, including compiling, using, and retaining the PII of Plaintiff and Class Members, while at the same time failing to maintain that information is secure from intrusion and theft by hackers and identity thieves.

152. Under principals of equity and good conscience, Defendant should not be permitted to retain the money it made from the use of the PII of Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

153. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable benefits and proceeds they received as a result of the conduct alleged herein.

**COUNT IV
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)**

154. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 96.

155. Defendant owes duties of care to Plaintiff and Class Members which requires Defendant to adequately secure their PII.

156. Defendant still possesses the PII of Plaintiff and Class Members.

157. Defendant does not specify in its Notice of Data Breach letter what steps they have taken to prevent this from occurring again.

158. Plaintiff and Class Members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

159. Plaintiff, therefore, seeks a declaration that (1) each of Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and Class Members, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

- a. Engaging third-party security auditors/penetration testers as well

as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring and identity theft restoration services for Plaintiff and Class Members for a period of ten years; and

h. Meaningfully educating Plaintiff and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class, request judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Class and appointing Plaintiff and her Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

- iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

- viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- ix. requiring Defendant to conduct regular database scanning and securing checks;
- x. purchasing credit monitoring and identity theft restoration services for Plaintiff and Class Members for a period of ten years
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs

discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated; and,
 - xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- D. For an award of damages, including actual, consequential, statutory, and nominal damages, as allowed by law in an amount to be determined;
 - E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
 - F. For prejudgment interest on all amounts awarded; and
 - G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: February 28, 2022

Respectfully Submitted,

/s/ Michael Hanna

Michael Hanna

MI Bar No. P81462

MORGAN & MORGAN

2000 Town Center, Suite 1900

Southfield, MI 48075

(313) 739-1950

mhanna@forthepeople.com

Jean S. Martin

Francesca Kester

MORGAN & MORGAN

201 N. Franklin Street, 7th Floor

Tampa, Florida 33602

(813) 559-4908

jeanmartin@ForThePeople.com

fkester@ForThePeople.com

*Attorneys for Plaintiff and the Proposed
Class*